

May 24, 2024

FILED IN CLERKS OFFICE

Honorable Magistrate Judge Hennessy
District of Massachusetts
Harold D. Donohue Federal Building and U.S. Courthouse
595 Main Street
Worcester, Massachusetts 01608

MAY 31 '24 PM2:18 USDC MA

Re: Re: Request to Publicize ***United States v. Kiejzo*** (20-mj-4234) Warrant and Warrant Affidavit

Criminal Case (CrC): 4:20-cr-40036-TSH

Magistrate Criminal Complaint Case (CC): 4:20-mj-04237-DHH

Magistrate Search Warrant Case (SWC): 20-mj-4234

Dear Judge Hennessy:

Thank you for responding to my initial letter docketed on Jan 22, 2024 (DN-10 SWC) by ordering the unsealing of case documents related to *United States v. Kiejzo* (DN-12 SWC). In this letter, I respectfully request that you reconsider the order to redact the Search Warrant Affidavit (SWA) and continued redaction of other documents that are part of the *Kiejzo* dockets. In your prior order (DN-12 SWC), you determined that specific paragraphs, 15-35, in the *Kiejzo* SWA (DN-5) should be redacted, continuing to shield specific text from the public because the United States indicated disclosing the text may compromise the government's interest in protecting information in "an ongoing criminal investigation. I disagree with the government's assessment to continue redaction and offer counterpoints for why redaction is unnecessary and not in the public's best interest. Because the same information is publicly accessible in this case and elsewhere, I am asking you to reconsider whether the redacted text in the *Kiejzo* SWA and other redacted documents does not prejudice the public's ability to access this case and the relevant information it contains. I do not believe the government has met their heavy burden necessary to overcome in their arguments to continue redaction.

The redacted text in the *Keijzo* SWA paragraphs 15-35 is already quoted elsewhere in the *Keijzo* case CrC.

For example in the instant criminal case, 4:20-cr-40036 DN-172 paradoxically has unredacted sections referring to the still redacted sections of the *Kiejzo* SWA (i.e., paragraphs 15-35 DN5 SWC), where sections of paragraphs or entire text from ¶15, 23, 31, 32, 33, and 34 are quoted (see appendix A for example text). DN-117 and DN-194 of the CrC also contain similar unredacted SWA text.

The text in the *Keijzo* SWA paragraphs 15-35 are publicly available in multiple, other similarly situated criminal court cases dealing with identical TARGET WEBSITES from

the same operation.

The *Kiejzo* SWA is not unique. It only differs from other, similar affidavits by combining two boilerplate affidavit templates for two separate TARGET WEBSITES into one, single affidavit. The U.S. Department of Justice (DOJ) Nationwide Investigation Advisory Committee (NIAC) created/help-create those two boilerplate SWA templates¹. The templates were developed in connection with a common operation for use by the government to apply to perform searches on properties suspected of accessing the TARGET WEBSITES (1) Hurt-meh and (2) BoyVids v4. I have attached three exhibits that show the TARGET WEBSITE SWAs contain identical boilerplate language. **Note, the common portions of all 3 documents were not highlighted in their entirety, just the first several pages relevant to the redacted paragraphs 15-35.**

- Exhibit 1 is the SWA from the instant case (DN-3-4 SWC) with some sections highlighted which are already publicly available, and/or identical to the other cases I reference.
- Exhibit 2 is an example Hurt-meh SWA and
- Exhibit 3 is a SWA from a BoyVids v4 case. *NOTE, the document is available completely unredacted from it's docket, the redactions were done to comply with Federal Rule of Crim. Proc. 49.1, which were not performed in that particular case before publication to the docket.

Each exhibit demonstrates that there is identical, and unredacted language used in the same way, in the same sections and yet the same text is redacted in the instant case. All three cases are part of the United States' Operation Jarvis and/or Operation Liberty Lane which were performed jointly with the Brazilian Operation Lobos 1 and U.K.'s NCA Operation Habitanca.

Additionally, it is unusual that the United States seeks to withhold boilerplate text specifically in the *Kiejzo* case because the government posed no objections in several nearly identical or similarly situated cases from the same operations; purportedly Operation Jarvis and Operation Liberty Lane in connection with Operation Lobos I. In those cases relating to Operation Jarvis and Operation Liberty Lane, the United States cited a lack of need to continue to seal or redact any information^{2,3} or failed to exercise any effort whatsoever to continue sealing in other districts⁴. For the same reasons, there is also no need to seal or redact the information in the instant *Kiejzo* case (i.e., *Kiejzo* SWA paragraphs 15-35).

Continuing to redact or seal the paragraphs in the *Kiejzo* SWA document is not only confusing to the carriage and consistency under the law, but limits the public's ability to understand the

¹ 2022-ICLI-00049 for example of Bateman template draft revisions being discussed

² *United States v. Corwin* 1:21-cr-121 (D.R.I.) Text Order 3/28/24 in addition to all cases that were automatically unsealed without public request being required.

³ *United States v. Delaney* 1:20-cr-00335, the Senior U.S. District Judge McAvoy unsealed numerous documents after two attorney's from the Department of Justice's Child Exploitation and Obscenity Section (CEOS) acknowledged that there were no longer reasons to seal certain exhibits and other information.

⁴ All SWA known from the E.D.Missouri have been fully unsealed without objections or motions by the government.

United States v. Kiejzo dealt with two TARGET WEBSITES (TARGET WEBSITE 2 and 3), which are Hurt meh⁵ and Boyvids v4.0⁶ according to other cases and government disclosures that were made available via FOIA and Brazil's Ministério Público Federal (MPF) or Federal Public Prosecutor's office. From FOIA disclosures and court records, there is evidence (see appendices) that the U.S. DOJ's (Nationwide Investigation Advisory Committee (NIAC⁷) drafted a boilerplate template for hundreds of Search Warrant affidavits in the United States, one for each of the multiple TARGET WEBSITES in operations Jarvis and Liberty Lane, which were derived from Operation Habitanca and Joint Operation Lobos which was derived from Joint Operation Baby Heart⁸. This information and its nexus to the instant case is evidenced by government disclosures and FOIA responses (see appendixes). The NIAC-made templates are nearly identical, which resulted in affidavits for search warrants that mainly differed by the only the description of which TARGET WEBSITE they were describing. The time period of the deanonymization is also narrowly constrained from March - June of 2019 and covered by NCA. TEI warrants, 91-TEI-0147-2019 and 91-TEI-0146-2019, so all of the affidavits mention dates of access during this time period using the same "tip" language from the NCA intelligence reports.

As a matter of constructive possession and collective organization in regards to the release of

8 <https://g1.globo.com/pe/paranagu%C3%A1/noticia/2021/12/03/pf-prende-pessoas-em-flagrante-e-cumpre-mandados-de-prisao-durante-operacao-contr-pornografia-infantil.ghtml>

information there is only one government.⁹ Further there is only one government in regards to the desire to keep the case sealed, despite it's many facets and agents, however the arguments have evolved over the past 4 years in federal districts that have (temporarily) permitted the cases to remain sealed or redacted. In other districts, there is no tolerance for such practices and the documents were promptly unsealed after the search warrants were executed.

When operations are individualized to a single district, this doesn't ordinarily present the public with such an opportunity to impeach the government's sealing or redacting arguments by comparing or contrasting different examples, but when the government's operation(s) spans multiple districts and countries, those arguments become vulnerable and ripe for refute in instances with uneven sealing practices and press releases.

Government's Evolving Arguments

In the government's initial motion to seal the *Kiejzo* documents, and keep them sealed, the government proffered that it didn't want to tip off any potential defendants.

"The government states that the public disclosure of any of these materials at this juncture could jeopardize the government's ongoing investigation in this case, specifically by giving the target subjects the opportunity to destroy evidence, both physician and digital." US v. Kiejzo 4:20-mj-04234 DN-1

This language was similar or identical in every district for the initial sealing of the search warrant case and all its related documents.

It is now several years later and the government has evolved two new reasons for concealing the text in paragraphs 15-35. In the *United States v. Delaney* Case (1:20-cr-00335-TJM DN-122) the government is quoted twice in these docketed attorney letters to the government's evolved reasons.

"After speaking with a CEOS trial attorney, I have been advised that there are currently other Project Jarvis cases pending litigation, and as such the government will continue to seek that certain matters remain sealed and/or redacted." U.S. v. Delaney 1:20-cr-00335-TJM DN-125 (N.D.N.Y)

Here, the government initially relied on a claim from a DOJ attorney that there

"are currently other . . . cases pending litigation." ([Delaney] Dkt. 97 at 4) Now, we are told that DOJ attorneys are claiming, for the first time and only after seeing our opposition in which we argued that a claim of pending litigation was insufficient, that there are "ongoing investigations of subjects suspected of

⁹ A common amalgamation of the opinions that effectively establish the principle that there is only one government with regards to discovery or information: *Kyles v. Whitley*, 514 U.S. 419 (1995), *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), *United States v. Bagley*, 473 U.S. 667 (1985)

accessing the website at issue." Dkt. 221 at 3. However, even now no explanation is given as to how public disclosure of the information could jeopardize these alleged investigations." U.S. v. Delaney 1:20-cr-00335-TJM DN-122 (N.D.N.Y)

However, if the government suggests that information from the *Delaney* case, which is identical to that in the *Kiejzo* instant case, could aid another defendant in demonstrating their innocence, this argument violates the other defendant's Fifth Amendment right to due process under the U.S. Constitution and prejudices the public. Any evidence from the *Kiejzo* instant case that shows or tends to show the innocence of any defendant, or indicates that their rights were violated, should have already been disclosed by the government in compliance with the requirements set forth in *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny.

The Due Process Protections Act (DPPA), signed into law on October 21, 2020, amended Rule 5 of the Federal Rules of Criminal Procedure. This amendment requires federal judges to issue a *Brady* order at the outset of every criminal case, reminding prosecutors of their obligation under *Brady v. Maryland* to disclose exculpatory evidence and specifying the potential consequences for failing to do so.

In this instant case, as in the previous case, the government prosecutors have shifted their argument (nationally in concert), citing "ongoing investigations." However, the government fails to explain how the information would impact these investigations and not merely affect other litigations, given that all tips provided by the FLA have been executed on, the TARGET SITES have long since ceased to operate or have been seized by the government, and the information is available in the public domain for those inclined to search for it. Five years have passed and the government has likely seized all evidence in connection with these tips, and that any ongoing investigation is protected by this fact. Furthermore, as the information is already public, the government bears the heavy burden of justifying continued secrecy, which cannot be met when not only is the the information public but clearly has a nexus¹⁰ to this case.

***Kiejzo* SWA paragraphs 15-35 are over-redacted, which goes against the best interests of the public.**

Regarding the continued Redacting of the SWA used in the United States' application of a search warrant, the public believes that the instant case continues to be "oversealed"¹¹ and over-redacted. The redacted sections of the *Kiejzo* SWA, which are paragraphs 15-35, have

¹⁰ Getting ahead of any arguments that the name of the TARGET WEBSITE was public known or other information was public but that the case was segregated from that public information by maintaining a level of secrecy, and being cryptic in the arguments and descriptions to avoid disclosure of the investigation into the TARGET WEBSITE or the individuals who allegedly utilized it.

¹¹ <https://www.justsecurity.org/78679/judicial-secrecy-how-to-fix-the-over-sealing-of-federal-court-records/>

already been disclosed to the public in other cases as well specific documents on the Keizo Criminal docket. It is in the public's interest to make the instant case information available because it prejudices any member of the public to be required to read multiple cases in different districts to piece together or comprehend the contents of the instant case. Further, any member of the public reading the instant *Kiejzo* case may not be aware that the entirety of the information is available elsewhere and place their reliance on good faith in the government and this Court to adjudicate what is and is not for public viewing.

Conclusion

Therefore, for the reasons that the sealed and/or redacted information is all, known and public. That the singular government's inconsistent arguments are dispelled in the face of this evidence; Because transparency and consistency in the law and legal proceedings is in the public's best interest, I respectfully ask the Court to reconsider the Order (*U.S. v. Kiejzo* 4:20-mj-04234 DN-12) on the matter of the redactions of the SWA affidavit and all other redactions made in the *Kiejzo* criminal case documents.

The redacted information is already known to the public and an established nexus of that public information exists between the instant case, it's redactions, and the other sources of said information.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read "Robert White". The signature is fluid and cursive, with the first letter of each word being capitalized and prominent.

Robert White
4949 Brownsboro RD #247
Louisville, KY 40222

UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

IN RE LETTER FROM A PUBLIC CITIZEN
ON THE ISSUE TO RECONSIDER MOTIONS
TO UNSEAL
SEARCH WARRANTS AND
REDACTED DOCUMENTS

20-mj-4234

UNITED STATES OF AMERICA

V.

VINCENT KIEJZO,

Defendant

Criminal No. 20-40036-MRG

The Court having received a subsequent letter to DN-12 asking for the unsealing and unredacting of documents and information having been heard by the court is GRANTED.

For the reasons:

The redacted information is already known to the public and an established nexus of that public information exists between the instant case and other Liberty Lane/Jarvis cases, it's redactions, and the other sources of said information.

Thus the Clerk is directed to UNSEAL/UNREDACT all documents filed under the protective order while observing the federal rules of criminal procedure 49.1 and relevant local rules to redact personal identifying information that could compromise the security or privacy of the individuals mentioned.

Appendix A

Instance Case examples of SWA text that is unredacted
4:20-cr-40036 DN-172

- “the Tor network attempts to [facilitate anonymous communication over the internet] by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a ‘circuit.’” Id. at ¶ 7.
- “available to internet users that is designed specifically to facilitate anonymous communication over the internet.” Id. at ¶ 7, 12.
- “online bulletin board dedicated to the advertisement and distribution of child pornography” that operated from at least September 2016 to June 2019. Id. at ¶ 15.
- “June of 2019, the computer server hosting Website 2, which was located outside of the United States, was seized by a foreign law enforcement agency.” Id. at ¶ 15.
- “an online forum dedicated to the sexual exploitation of minor and/or prepubescent males.” Id. at ¶ 23
- “the computer server hosting Website 3, which was located outside of the United States, was seized by a foreign law enforcement agency.” Id. at ¶ 23
- “In August 2019, a foreign law enforcement agency (hereinafter, “FLA”) known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that the FLA had determined that on May 12, 2019 at 19:10:51 UTC, IP address 96.230.213.63 was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 2. Id. at ¶ 31.
- “[u]sers were required to create an account (username and password) in order to access the majority of the material” ¶ 31.
- “FLA provided further documentation naming the site...as Website 2” ¶ 31.
- “In August 2019, FLA notified U.S. law enforcement that FLA had determined that on May 12, 2019 at 19:27:24 UTC, IP address 96.230.213.63 was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 3.” Id. at ¶ 32
- “an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys.” Id. at ¶ 32
- “users were able to view some material without creating an account,” but that “an account was required to post and access all content. Id. at ¶ 32
- “national law enforcement agency of a country with an established rule of law.”
- “long history of U.S. law enforcement sharing criminal information with FLA and FLA sharing criminal investigation information with U.S. law enforcement.” Id. at ¶ 33.
- “had obtained that [tip] information through independent investigation that was lawfully authorized in FLA’s country pursuant to its national laws.” Id. at ¶ 33
- “advised U.S. law enforcement that FLA had not interfered with, accessed, search or seized any data from any computer in the United States in order to obtain that IP address information.” Id. at ¶ 33

- (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession. Id. at ¶ 34

4:30-cr-40036 DN-117

- The affidavit stated that in June 2019, the computer server hosting those websites, which was located outside the United States, was seized by a foreign law enforcement agency ("FLA"). Id. at ¶ 15, 23
- "used to access online child sexual abuse and exploitation material via ... website[s] that the FLA named and described as Website[s] 2 [and 3]"
- "notified U.S. law enforcement that the FLA had determined that on May 12, 2019... [the IP address] was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 2 [and 3]." Exhibit F at ¶ 31, 32

4:20-cr-40036 DN-194

- on May 12, 2019 at 19:10:51 UTC, [IP address] was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 2. FLA . . . stated that users were required to create an account (username and password) in order to access the majority of the material, and provided further documentation naming the website as Website 2, which the FLA referred to by its actual name
- On 2019-05-12 19:10:51 (UTC) [IP address] was used to access online child sexual abuse and exploitation material [description omitted]. Users were required to create an account (username and password) in order to access the majority of the material[.]

Appendix B

Information released

This is not an exhaustive list of the defendant's nor of the information released, nor is it every citation. As the public has a right to the information, it is prejudicial to the public to resort to documenting each instance the information has been released and provide it to prove a right to the information. The government bares the burden of keeping the information sealed/redacted. Some of the information has been liberated from transparent districts that automatically unseal documents if the government does not file a motion to continue sealing every 6 months. There is only one government. Once information is made public, to continue sealing it makes little sense, likening it to "putting the toothpaste back in the tube" or the "opening of Pandora's box".

1. There were at least two or more FLAs¹², not one as reported in the SWA..
 - a. National Crime Agency¹³ of the United Kingdom¹⁴ was an FLA
 - b. Federal Police of Brazil was an FLA¹⁵
 - c. Germany was a partner in the operation¹⁶
2. The U.S. FBI and U.S. HSI worked with Brazil's Federal Police and the United Kingdoms NCA¹⁷ as part of Operation Lobos 1 to locate the server, shut it down, arrest the System Administrator, and obtain the contents of the Server. This is after the Operation Baby Heart was conducted Jointly with Portugal, and others. The number of partners is expected to include the entire roster of the Virtual Global Taskforce (VGT)¹⁸.
3. There were at least 8 Websites as part of this operation.
4. 5 Websites that were reported on the Brazilian server.
 - i) **Baby Heart**¹⁹
 - ii) **Hurt-meh**²⁰
 - iii) **Boy-Vids**²¹ -Other defendants that were alleged to have visited that site as part of the same operation as the defendant, re

12 1:19-CR-10012 US v. Bateman

13 *United States v. Delaney* 1:20-cr-335 DN-46-1 (N.D.N.Y.)

14 *United States v. Burton* 4:21-cr-03020 DN-56 (D. Neb.) (said Law Enforcement from England), *US v. Shacar* 3:21-cr-30028 DN-103 (D.Mass.)

15 (Brazilian MPF press release) via aNPR - *United States v. Stuart* 21-CR-07 DN-100-4 (W.D.N.Y.)

16 FOIA Response - 2022-ICLI-00049

17 (Brazilian MPF press release)

18 see <https://nationalcrimeagency.gov.uk/virtual-global-taskforce> (founded by Home Land Security Investigations (HSI), currently operated by the NCA)

19 Brazilian MPF press release, *United States v. Bates* 3:22-mj-01074 (D. Conn.), *United States v. Daily* 3-21-cr-00118 (W.D.K.Y.), *United States v. Diehl* 4:22-cr-00055 (E.D.M.O.), *Stuart*, and others

20 Brazilian MPF press release, *US v. Corwin* 2:21-cr-218 DN-36 (E.D.N.Y.), *United States v. Stauffer* 4:20-mj-4005 DN-1 (S.D. Ill.) and others

21 Brazilian MPF press release, *Delaney* at DN-46-5, *United States v. Premises (Bradley)* 1:20-MJ-00255 (E.D.M.O.), *United States v. Clemence* 1:21-cr-00099 (D.N.H.), *United States v. Premises (Hammons)* 4:20-mj-05049 DN-1 (E.D.M.O.), and others

iv) **Forbidden Angels AKA Anjos Proibidos**²²

v) **Loli Lust**²³

5. The Website Girland²⁴
6. Existence of one or more intelligence reports received from the NCA²⁵
7. The FBI already had a documented preliminary investigation into a TOR hidden service operating on the same server as Delaney's TARGET WEBSITE as of January 13, 2017.
8. The date each TARGET WEBSITE was brought online²⁶
 - a. Baby Heart Oct. 2016²⁷, Hurt-meh July 1st, 2016, Boy Vids 4.0 2013,
9. The date each TARGET WEBSITE went offline²⁸ (example: June 6, 2019)
10. The number of postings for each TARGET WEBSITE²⁹. (example: 81,000 postings)
11. Number of Members for each Target Website^{30,31}, both during the operation, and when the websites went offline (example 820,000 members for Hurt-meh, 310,000 for BoyVids 4.0³²)
12. TARGET WEBSITE DESCRIPTION for the *DELANEY* CASE:
 - a. "web site that facilitated the sharing of child sex abuse and exploitation material with a particular emphasis on indecent material of young boys"
 - b. "Users of the website were able to view some material without creating an account. However, an account was required to post and access all content."
13. The number of alleged accesses for the particular IP address alleged in the TIP³³
14. Quoted Postings from the TARGET WEBSITES
15. Board Rules for each TARGET WEBSITE
16. Subforums located within the TARGET WEBSITES
17. Type of site the TARGET WEBSITE consisted of (chatsite, forum, board, image server)
18. Names of the agents at the Headquarters which prepared and approved the investigative reports sent to field offices³⁴
19. Project Jarvis³⁵, Project Habitanca³⁶, Operation Liberty Lane^{37,38,39}, Operation Lobos⁴⁰

22 Brazilian MPF press release

23 Brazilian MPF press release

24 *Shacar* DN-113

25 *Delaney* DN-46*

26 *Washington State v. Albert Dykes* 2:21-00380-04 DN-2

27 *Hunting Lodge* SWA

28 *Search of Hunting Lodge* 1:20-mj-00243-LPA

29 *United States v. SEARCH WARRANT* (Duffy) 5:20-mj-44 DN-2 (N.D.Fla.)

30 *Hammons* SWA

31 *Hunting Lodge* SWA

32 *Hammons* SWA

33 *United States v. In Re: 54 Spruce St., Apartment 6, Burlington, VT (Keve)* 2:20-mj-00143-kjd SWA

34 *Delaney* FBI report DN-136

35 *Delaney* FBI Report DN-136

36 Available at Wikipedia article "Project Habitanca", as well as FOIA response 2022-ICLI-00049

37 *United States v. White* 3:21-cr-155 DN31-1 available on Courtlistener at

<https://storage.courtlistener.com/recap/gov.uscourts.kywd.123856/gov.uscourts.kywd.123856.31.1.pdf>

and DN-75-1 available on Courtlistener at

<https://storage.courtlistener.com/recap/gov.uscourts.kywd.123856/gov.uscourts.kywd.123856.75.1.pdf>

38 FOIA Response 2022-ICLI-00049

39 Reddit Thread : [https://preview.redd.it/f42v8c6r6mdc1.png?](https://preview.redd.it/f42v8c6r6mdc1.png?width=621&format=png&auto=webp&s=c8c7045eb92417161dd05794e8ed757975a110dd)

[width=621&format=png&auto=webp&s=c8c7045eb92417161dd05794e8ed757975a110dd](https://preview.redd.it/f42v8c6r6mdc1.png?width=621&format=png&auto=webp&s=c8c7045eb92417161dd05794e8ed757975a110dd)

40 Brazilian MPF press release and Wikipedia article

Standard case information released information released:

1. Alleged IP address
2. Alleged UTC time of access
3. Alleged Date of access
4. Month the FBI received the TIP from the FLA - being August for 5 of the websites.
5. Description of the TARGET WEBSITE(s)
6. File names, and descriptions of images alleged to have been on (or actually URL linked from) the TARGET WEBSITE(s)
7. Names of search/case agents involved in the search and seizure.
8. Type of Browser used by the defendant: TOR project browser or Opera for example⁴¹
9. Number and description of the total alleged CSAM found and 404b evidence the defendant was alleged in possession of
10. Indictment (with the grand jury foreperson's name redacted)
11. "Notice of Forfeiture" OR alternatively "Allegation of Forfeiture"
12. Criminal Complaint or Information Document
13. Stipulation of Facts (as part of plea agreements)
14. Username(s) that the defendant allegedly used⁴²
15. The name of the Internet Service Provider in each case
16. The Date the search warrant was signed
17. The date the search warrant was executed
18. Unredacted executed search warrants including the list of seized items
19. Any prior history with law enforcement (whether it was sustained or not, or sealed)
20. Government investigative report on the subject including:⁴³
 - a. NCMEC search
 - b. NCIS search
 - c. National sex offender registry search
 - d. DMV search
 - e. ICACCOPS database search
 - f. Accurant Search
 - g. Social Media Searches
 - h. Employment searches
 - i. Copy
21. Copy of the Subpoena sent to the ISP and the response.

⁴¹ *United States v. Thomas Clark* 2:21-mj-00147 DN-1 (W.D Wash.) Criminal Complaint

⁴² *Stauffer* DN-1

⁴³ *Delaney* DN-46

Example of additional document with Excessive Redaction in Kiejzo case

Excessive Redaction in 172 of the Kiejzo Criminal Docket

- Page 2 footnote 2 - Website name is **Hurt meh** as described in document with exact matching description has already been released by the government.
- Page 3 footnote 3 -Website name **Boyvid 4.0** as described in document with exact matching description has already been released by the government.
- Page 4 redacted section referring to the National Crime Agency of the United Kingdom has already been released by the government in the following cases:
- Page 6 redacted sections referring to the National Crime Agency (NCA)
- Page 6 redacted sections referring to the United Kingdom
- Page 6 redacted sections referring to website 2 Hurt Meh
- Page 6 redacted section referring to NCA
- Page 8 redacted section referring to NCA or Brazilian Federal Police
- Page 16 redacted sections referring to NCA
- Page 17 redacted sections referring to NCA
- Page 18 redacted sections referring to the NCA intelligence report which has been made public in the Delaney Case.
- Page 18 redacted website description that is unredacted in these other cases.
- Page 19 redacted sections referring to the NCA
- Page 20 redacted sections referring to the NCA
- Page 21 redacted sections referring to the NCA and/or Brazil
- Page 22 redacted sections referring to NCA and/or Brazil
- Page 23 redacted section referring to NCA and/or Brazil
- Page 24 redacted section referring to NCA and/or Brazil
- Page 29 redacted section referring to Hurt Meh
- Page 30 redacted section referring to Babyheart, or Hurt Meh
- Page 31 redacted sections referring to NCA or Brazilian Police
- Page 32 redacted sections referring to Hurt Me or Boyvids 4.0
- Page 33 redacted sections referring to NCA

EXHIBIT “1”

4:20-mj-04234

4:20-mj-04234-DHH - Redacted Search Warrant Affidavit with paragraphs 15-35 redacted. Relevant sections highlighted that are common to Exhibit 2 and Exhibit 3, the “Hurt-meh” SWA and “Boyvids v4”SWA respectively.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Caitlin Moynihan, a Special Agent with Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Homeland Security (“DHS”), Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), and am assigned to the office of the Special Agent in Charge, Boston, MA. I have been a Special Agent since October 2009. Prior to being assigned to the SAC Boston Office, I was assigned to the Resident Agent in Charge Office in Burlington, Vermont. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of 18 U.S.C. §§ 2422, 2423, 2251, and 2252A. I have received training in the investigation of child exploitation offenses, including child pornography, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).
2. I submit this affidavit in support of an application to search the premises located at ■ Joan Circle, Milford, Massachusetts 01757 (the “SUBJECT PREMISES”), as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.
3. The statements in this affidavit are based in part on information provided by federal agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement

20-mj-4234-DHH

agencies; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by federal agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with HSI.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Attempted Receipt of Child Pornography) and 2252A(a)(5)(B) and (b)(2) (Access with Intent to View and Possession of Child Pornography, and attempt) are located at the SUBJECT PREMISES.

BACKGROUND OF THE INVESTIGATION

5. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via hidden service websites that operated on the Tor anonymity network. The websites are described below and referred to herein as “Website 2” and “Website 3.”¹ There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed Website 2 and Website 3, as further described herein.

¹ The names of Website 2 and Website 3 are known to law enforcement. Investigation into the users of the websites remain ongoing and disclosure of the names of the websites would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

The Tor Network

6. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses,² which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.
7. **Website 2** and **Website 3**, further described below, operate or operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

² An "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

8. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free “Tor browser” from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.³ The Tor browser is a web browser that is configured to route a user’s Internet traffic through the Tor network.
9. As with other Internet communications, a Tor user’s communications are split into packets containing header information and a payload and are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user’s IP address with Tor network relay computers, which are called “nodes.” This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.
10. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user’s communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an Internet website, only the IP address of the last relay computer (the “exit node”), as opposed to the Tor user’s actual IP address, appears on that website’s IP address log. In addition, the content of a Tor user’s communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor

³ Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

node from observing the content (but not the routing information) of other Tor users' communications.

11. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is in bold text, "**No.**"
12. The Tor Network also makes it possible for users to operate websites, such as **Website 2** and **Website 3**, that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.
13. Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a

20-mj-4234-DHH

Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

14. Hidden service websites on the Tor Network are not “indexed” by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Users utilize those directory sites to identify new web forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children. While they operated, the web addresses for **Websites 2 and 3** were listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

Website 2

15.

[REDACTED]

[REDACTED]

20-mj-4234-DHH

16.

[REDACTED]

17.

[REDACTED]

18.

[REDACTED]

20-mj-4234-DHH

19.

20.

21.

20-mj-4234-DHH

[REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

22. [REDACTED]

[REDACTED]

20-mj-4234-DHH

[REDACTED]

a.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

4

[REDACTED]

20-mj-4234-DHH

b. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

c. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

20-mj-4234-DHH

[REDACTED]

Website 3

23.

[REDACTED]

24.

[REDACTED]

20-mj-4234-DHH

25.

[REDACTED]

26.

[REDACTED]

27.

[REDACTED]

28.

[REDACTED]

20-mj-4234-DHH

29.

a.

b.

c.

20-mj-4234-DHH

[REDACTED]

Evidence Related to Identification of Target that Accessed Website 2 and Website 3

30. [REDACTED]

31. [REDACTED]

20-mj-4234-DHH

32.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

33.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20-mj-4234-DHH

34.

[REDACTED]

35.

[REDACTED]

20-mj-4234-DHH

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

36. I am also aware through consultation with HSI and FBI agents that the review of detailed user data related to one Tor network based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account.
37. Accordingly, based on my training and experience and the information articulated herein, because accessing **Website 2** and **Website 3** required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web addresses for **Website 2** and **Website 3**, and then connecting to **Website 2** and **Website 3** via Tor – it is extremely unlikely that any user could simply stumble upon **Website 2** or **Website 3** without understanding their purpose and content.
38. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed **Website 2** and **Website 3** has, at a minimum, knowingly accessed **Website 2** and **Website 3** with intent to view child pornography or attempted to do so.

Identification of SUBJECT PREMISES

39. According to publicly available information, IP address 96.230.213.63 — the one used to access **Website 2** and **Website 3**, as described above — is owned/operated by Verizon Fios. On or about March 20, 2020, an administrative subpoena was issued to Verizon Fios for information related to IP address 96.230.213.63 on the following dates and times: May 12, 2019 at 19:10:51 UTC and May 12, 2019 at 19:27:24 UTC, respectively. Verizon Fios provided the following subscriber details for the IP address on those dates:

Customer name:	[REDACTED]
Account address:	Joan Cir Milf (sic), MA 01757 (the SUBJECT PREMISES)
Account Creation Date:	08/31/2012
Status:	Active

40. Commercial databases indicate that [REDACTED] resides at the SUBJECT PREMISES. A query of the Worcester Registry of Deeds website indicated the SUBJECT PREMISES has been owned by [REDACTED] since 1994. Open source research indicates that it is a single-family home.
41. Records from the Massachusetts Registry of Motor Vehicles (RMV) as of June 2020 show that [REDACTED], [REDACTED] and Vincent Kiejzo (YOB 1987) all have active Massachusetts driver's licenses, each of which includes a photograph and designation of the SUBJECT PREMISES as their residential address.
42. Through consultation with the United States Postal Service (USPS), agents confirmed that the residents currently receiving mail at the SUBJECT PREMISES bear the names [REDACTED] and Vincent Kiejzo.⁵

⁵ Additional record checks suggest that [REDACTED] currently resides out of state in Oregon.

20-mj-4234-DHH

43. On September 4, 2020, agents conducting surveillance at the SUBJECT PREMISES observed a man matching the likeness of the male depicted in the RMV photograph of [REDACTED] depart the residence on foot at approximately 6:45 a.m.
44. On September 8, 2020, agents conducting surveillance at the SUBJECT PREMISES observed a man matching the likeness of the male depicted in the RMV photograph of Vincent Kiejzo departing the SUBJECT PREMISES at approximately 6:30 a.m., operating a [REDACTED] 2020 Acura RDX, MA REG [REDACTED].⁶ Agents observed this same vehicle parked at Memorial Elementary School in Milford at approximately 7:25 a.m.
45. According to the Milford Police Department, Vincent Kiejzo was issued a Firearms Identification Card in May 2017 which includes designation of the SUBJECT PREMISES as his residential address. There are seven firearms registered to Vincent Kiejzo.
46. Through open source research, agents located a LinkedIn page for Vincent Kiejzo which lists his employment from 2013 to the present as a second grade teacher at Milford Public Schools. The LinkedIn page also listed employment from 2017 with a position of Co-Founder/President of Milford Massachusetts Foundation for Education, Inc. Additionally, the following employments are listed on the LinkedIn profile: pool supervisor/swimming lesson supervisor at Milford Community School Use Program, with employment dates of 2001 to the present; elementary instructional technology specialist at Milford Public Schools, with employment dates of 2012-2013; and one-to-one behavior specialist at Milford Public Schools, with employment dates of 2008 to 2012. The male depicted in the picture on the LinkedIn profile appears to match the likeness of the male depicted in the

⁶ The Acura is registered to Honda Lease Trust of Holyoke, MA.

RMV photograph of Vincent Kiejzo. Publicly accessible websites associated with Milford schools also show Vincent Kiejzo as a second grade teacher.

47. On September 2, 2020, I traveled to the SUBJECT PREMISES and used an openly available wireless network discovery tool to search for available wireless networks, while parked in front of the SUBJECT PREMISES. This produced two wireless networks in the area, both secured, which appeared to be associated with the SUBJECT PREMISES: named KIEJZO and KiejzoSH.

CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

48. Based on my previous training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create, possess, receive, distribute, or access with intent to view child pornography (collectively, “consumers” of child pornography) have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to such consumers of child pornography, as outlined in the following paragraphs.
49. The majority of consumers of child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
50. Consumers of child pornography may collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics, or digital or other images for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the

level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

51. Many consumers of child pornography maintain their sexually explicit materials for several years and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They regularly maintain their collections in the privacy and security of their homes, inside their cars, on their person, or in cloud-based online storage. Depending on their technical expertise, access to child pornography on seemingly “safe” networks like Tor, or struggle with addiction to child pornography, many consumers of child pornography have been found to download, view, and then delete child pornography on their digital devices on a cyclical and repetitive basis.
52. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.⁷

⁷ See United States v. Carroll, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also United States v. Seiver, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., United States v. Allen, 625 F.3d 830, 843 (5th Cir. 2010); United States v. Richardson, 607 F.3d 357, 370-71 (4th Cir. 2010); United States v. Lewis, 605 F.3d

53. Consumers of child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. Furthermore, individuals who would have knowledge about how to access a hidden and embedded chat site would have gained knowledge of its location through online communication with others of similar interest. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, bulletin boards, chat sites, web forums, instant messaging applications, and other similar vehicles of communication.
54. Consumers of child pornography often collect, read, copy, or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in written hardcopy, on computer storage devices, or merely on scraps of paper.
55. Based upon training and experience, I know that persons engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

395, 402 (6th Cir. 2010)).

20-mj-4234-DHH

56. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that he possesses or controls. Additionally, based on this training and experience, I understand that even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).
57. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to consumers of child pornography. In particular, the target of this investigation obtained and used Tor network software, found the web addresses for **Website 2** and **Website 3**, and accessed online child sexual abuse and exploitation material via **Website 2** and **Website 3**. In my experience, individuals who rely on access to materials depicting the sexual abuse of children through the Tor network tend to have sophisticated expertise with computers and they are typically individuals who are taking steps to hide their viewing of child exploitation materials.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

58. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:
- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
 - b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.
 - c. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a

20-mj-4234-DHH

digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

- d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- e. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
- f. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic

communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

59. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
60. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, accessing the internet, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.
61. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:
62. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto

a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

63. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
64. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.
65. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” An internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

66. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or

20-mj-4234-DHH

storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an

20-mj-4234-DHH

incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

67. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
68. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
69. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on

- a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
70. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.
71. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:
- a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to

examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

- b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

- 72. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things

described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

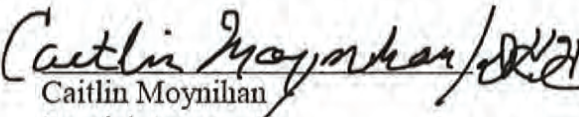
73. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.
74. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.
75. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical

20-mj-4234-DHH


experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CONCLUSION

76. Based on the foregoing, I submit there is probable cause to believe that violations of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Attempted Receipt of Child Pornography) and 2252A(a)(5)(B) and (b)(2) (Access with Intent to View and Possession of Child Pornography, and attempt) have occurred, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES as described in Attachment A, authorizing the seizure and search of the items described in Attachment B.


Caitlin Moynihan
Special Agent
Homeland Security Investigations

Sworn and subscribed before me telephonically pursuant to Fed. R. Crim. P. 4.1 this 8th day of September, 2020. 5:21 p.m.


HONORABLE DAVID H. KENNEDY
United States Magistrate Judge




EXHIBIT “2”

4:20-mj-04234

1:19-mj-00830-DJS N.D.N.Y 2019 - Redacted “Hurt Meh” Search Warrant Affidavit with redactions per Federal Rules of Criminal Procedure 49.1. Relevant sections highlighted that are common to Exhibit 1, the “*Kiezjo*” SWA.

UNITED STATES DISTRICT COURT

for the

HURTMEH BOILERPLATE AFFIDAVIT

Eastern District of Missouri

In the Matter of the Search of
PREMISES LOCATED AT: [REDACTED] Crimson Lane, Barnhart Missouri, 63012 within
the Eastern District of Missouri, a two-story structure with a tan siding and tan brick
exterior, with black shutters, a three (3) car garage and a shingle-style roof. The
numbers "[REDACTED]" are clearly displayed on the front porch post.
(SEE ATTACHMENT A.)

Case No. 4:20 MJ 3301 NCC
FILED UNDER SEAL
SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Special Agent Daniel Root, FBI, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:
SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

21, USC, § 2252(a)(2) and (b)(1)
21, USC, § 2252(a)(4)(b) and (b)(2)

Offense Description

receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct
possession of and access with intent to view a visual depictions of a minor engaged in sexually
explicit conduct

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.



11/12/2020

Applicant's signature

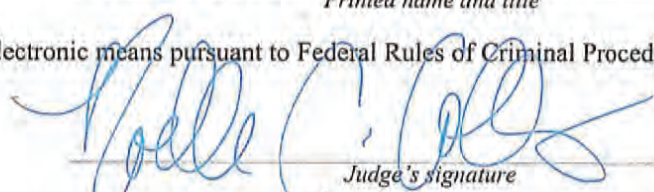
Special Agent Daniel Root, FBI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 40.

Date: November 12, 2020

City and state: St. Louis, MO



Judge's signature

Honorable Noelle C. Collins, U.S. Magistrate Judge

Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF:)
PREMISES LOCATED AT: [REDACTED] Crimson)
Lane, Barnhart Missouri, 63012 within the)
Eastern District of Missouri, a two-story)
structure with a [REDACTED] siding and [REDACTED] brick)
exterior, with [REDACTED] shutters, a [REDACTED] car)
garage and a shingle-style roof. The numbers)
"[REDACTED]" are clearly displayed on the front porch)
post.)
(SEE ATTACHMENT A.))

No. 4:20 MJ 3301 NCC

FILED UNDER SEAL

SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Root, a Special Agent with the Federal Bureau of Investigation being duly sworn,
depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) since January 2016, and am currently assigned to the St. Louis Division. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training provided by the FBI and through everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. During my time as a case agent on numerous complex investigations, I utilized a variety of investigative techniques to include: organizing and participating in physical surveillance; participating in undercover operations; serving search warrants; making arrests; and interviews involving defendants. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at [REDACTED] Crimson Lane, Barnhart, Missouri (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § § 2251, 2252, and 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:
- a. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign

commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

- b. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
- c. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
- d. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.
- e. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or

transported in or affecting interstate or foreign commerce by any means, including by computer.

- f. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

- a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.
- b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

- c. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.
- d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
- e. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- f. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.
- g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).
- h. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices);

peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

- i. “Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone” as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- j. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- k. The “Domain Name System” or “DNS” is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.
- l. “Encryption” is the process of converting data into a code in order to prevent unauthorized access to the data.
- m. A “hidden service,” also known as an “onion service,” is website or other web service that is accessible only to users operating within the Tor anonymity network.
- n. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- o. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- p. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- q. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.
- r. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

- s. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form
- t. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- u. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.
- v. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.
- w. The “Tor network” is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.”
- x. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.
- y. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- z. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language

(HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the “TARGET WEBSITE.”¹ There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet’s source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.
8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.” Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

¹ The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free “Tor browser” from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.² The Tor browser is a web browser that is configured to route a user’s Internet traffic through the Tor network.
10. As with other Internet communications, a Tor user’s communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user’s IP address with Tor network relay computers, which are called “nodes.” This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.
11. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user’s communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the “exit node”), as opposed to the Tor user’s actual IP address, appears on that website’s IP address log. In addition, the content of a Tor user’s communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users’ communications.
12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user’s actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user’s communications totally anonymous. For example, in the Tor Project’s FAQ, the question “So I’m totally anonymous if I use Tor?” is asked, to which the response is, in bold text, “No.”

² Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

13. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called “hidden services” or “onion services.” They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server’s location.
14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example “asdlk8fs9dfku7f,” followed by the suffix “.onion.” Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System (“DNS”) listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users’ computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Target Website 2: Hurt-Meh

Description of TARGET WEBSITE

15. The TARGET WEBSITE was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, the computer server hosting the TARGET WEBSITE, which was located outside of the United States, was seized by a foreign law enforcement agency.
16. A review of the initial TARGET WEBSITE page revealed it was a message board web page that contained a search bar, and showcased two hyperlinks titled, “Announcements” and “Important Information.” Located below the title were hyperlinks including those entitled

“Quick Links,” “Home,” “Board Index,” “Login,” and “Register.” As of June 2019, the website had over 820,000 members and over 81,000 postings.

17. Upon accessing the “Announcements” hyperlink of the TARGET WEBSITE, the following message was displayed in message board form, “Welcome, Please read before registering” which was dated July 1, 2016. Upon accessing the aforementioned hyperlink, the message read, “Welcome abusers and abusees and those that enjoy watching. This website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such.” Based on my training and experience, I know that Hurtcore refers to violent pornography. The message continued, “PS Please register to see all the forums, and use strong password for user profile.”
18. Upon accessing the “Register” link of the TARGET WEBSITE, it was revealed that users would complete a “Username,” “Password,” “Confirm password,” “Language,” and “My timezone,” fields, as well as a “Confirmation of Registration” code. Upon entering the TARGET WEBSITE, sections and forums for posting to the website included “HURTCORE Toddlers Videos (Ages 0-5),” “Preteen/Hebe Children Videos (Ages 6-13),” “Teens Videos (Ages 14+),” “Toddlers Images (Ages 0-5),” “Preteen/Hebe Children Images (Ages 6-13),” and “Teens Images (Ages 14+).” Based on my training and experience, I know that “Hebe” is a reference to a “hebephile,” which is a person with a persistent sexual interest in pubescent minor children. Another forum was named “GORE/DEATH” which included sub-forms for “Toddlers (Ages 0-5),” “Preteen/Hebe Children (Ages 6-13)” and “Teens (Ages 14+).” An additional section of the website called “The Team” listed the usernames of two website “Administrators” and five “Global Moderators.” The TARGET WEBSITE also contained a private message feature that was available, allowing users to send private messages to each other.
19. On June 23, 2016, a website administrator posted a topic entitled “Board Rules” in the “Important Information” forum which contained the following explanation of the website:
Rules are simple all material must be related to Hurtcore content. What is Hurtcore content? It is rape, fighting, wrestling, bondage, spanking, pain, mutilation, gore, dead bodies, and etc. (no limits) Why does this place exist? There was a need and since society thinks I am worst than any abuser or creator of Hurtcore content, I decided to create this place for those who like

it and want to share. Besides I am the mischievous god. It is up to you to make this the best Hurtcore board there is. So please upload whatever you can so that it can be shared.

20. A review of the “Toddlers Videos,” “Preteen/Hebe Children,” “Toddlers Images,” and “Gore/Death” forums and subforums, as well as additional forums, within the various above sections revealed they contained numerous pages of topics. Each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the thread below it. Typical posts appeared to contain text, images, thumbnail previews of images, links to external sites with compressed files (such as “.rar”), or replies to previous posts.
21. A review of topics within these sections revealed numerous posts containing images and/or videos depicting child pornography and child erotica of prepubescent males, females, toddlers, and infants; including those depicting anal, vaginal, and oral penetration. Additionally, these sections revealed numerous posts containing images and/or videos depicting child pornography involving gore and sometimes death. Examples of these are as follows:
22. On October 9, 2016, a website user posted a topic entitled “Fuck the newborn. Real fuck!” in the “Hurtcore/Toddlers Images/Girls” forum that contained nine images depicting child pornography and child erotica of a prepubescent female infant. One of these images depicted a naked female infant lying on her back with her legs spread apart, exposing her vagina, with a gloved adult finger inserted into her anus. A male’s penis was pressed against her vagina and the head of the penis inserted into her mouth. A brown liquid substance, appearing to be the infant’s feces are seen smeared around her anus.
23. On November 5, 2016, a website user posted a topic entitled “BabyHee 1yo (one of full version)” in the “HurtCore/Toddlers Videos/Boys” forum that contained images depicting child pornography and torture of a prepubescent male, who was completely naked and tied down with rope on the side of a bath tub. Among other things, the images depicted an adult male defecating on the chest and urinating in the mouth of the prepubescent male.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

24. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.
25. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on May 24, 2019, IP address 76.253.61.232 "was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE. FLA described the website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children," stated that "[u]sers were required to create an account (username and password) in order to access the majority of the material," and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name.
26. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law

enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

27. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.
28. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on

Paragraph 14 in Kiejzo Case: 4:20-mj-4234

one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

29. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.
30. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

Identification of SUBJECT PREMISES

31. On May 24, 2019, TARGET WEBSITE was accessed at 01:34:38 UTC from IP address 76.253.61.232.
32. According to publicly available information, IP address 47.24.167.115 was owned/operated by AT&T Communications, Inc.
33. On November 22, 2019, an administrative subpoena was issued to AT&T in regard to the pertinent IP address. A review of the results obtained on November 25, 2019, identified the following account holder and address:

Name: [REDACTED]
Address: [REDACTED] Crimson Lane Barnhart, MO 63012
Telephone: [REDACTED]

34. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for [REDACTED] Crimson Lane, Barnhart, MO. This search revealed that [REDACTED] Crimson Lane, Barnhart, MO was a single family residence, owned by **Brent M. and [REDACTED]**. These public records indicated that **BRENT M. LAWSON**, date of birth [REDACTED]/1976, and [REDACTED], date of birth xx/xx/70 currently reside at the SUBJECT PREMISES and that they have owned/lived at this address since April of 2015.

35. A check with the Department of Motor Vehicles on or about August 19, 2020, revealed that BRENT LAWSON'S driver's license lists the SUBJECT PREMISES as his current address, and he has a vehicle registered with the State of Missouri that he owns and that is also registered to the SUBJECT PREMISES.
36. On or about August 13, 2020, a representative from Ameren indicated that electric service is currently being provided to BRENT LAWSON at the SUBJECT PREMISES.
37. Surveillance of the SUBJECT PREMISES on or about August 18, 2020, identified a [REDACTED] Toyota Highlander bearing Missouri license plate [REDACTED], parked in the driveway in front of the residence, and a [REDACTED] GMC Yukon bearing Missouri license plate [REDACTED] also parked in the driveway. The Toyota Highlander was determined to be registered to [REDACTED]. The GMC Yukon was determined to be registered to BRENT LAWSON.
38. Further research indicated that BRENT MICHAEL LAWSON is a registered sex offender per records maintained by the Missouri State Highway Patrol. His address is listed in the sex offender registry as [REDACTED] Crimson Lane, Barnhart MO, for both work and home addresses. Vehicles registered to him on the sex offender registry are a 2004 Yukon with plate [REDACTED], a 2019 Kia with plate [REDACTED] and a 2017 Highlander with plate [REDACTED]. According to public records available via the Public Access to Court Electronic Records (PACER) website, his obligation to register stems from a conviction on April 22, 2004, in the U.S. District Court for the E.D. of Missouri, for the offenses of Transportation of Child Pornography in violation of Title 18, United States Code, Section 2252(a)(1); Attempted Receipt of Child Pornography in violation of Title 18, United States Code, Section 2252A(a)(2); and Possession of Child Pornography in violation of Title 18, United States Code, section 2252A(a)(5)(B), for which BRENT MICHAEL LAWSON, was sentenced by the Hon. Judge Stephen N. Limbaugh to sixty months of imprisonment followed by three years of supervised release.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

39. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or

smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

40. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).

41. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

- a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
 - c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
 - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
44. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as

the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an

incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or

received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

45. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading

filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

46. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator’s network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.
47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require

techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

48. This warrant permits law enforcement to compel **BRENT MICHAEL LAWSON** to unlock any DEVICES owned or used by him requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:
- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
 - b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
 - c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that

match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.
- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when

the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.


- h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of **BRENT MICHAEL LAWSON** to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of **BRENT MICHAEL LAWSON** and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of **BRENT MICHAEL LAWSON** and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that **BRENT MICHAEL LAWSON** state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel **BRENT MICHAEL LAWSON** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

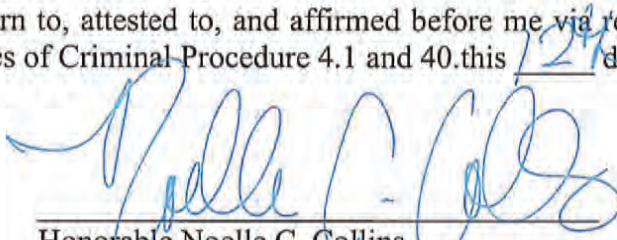
50. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

I state under the penalty of perjury that the foregoing is true and correct.

 11/12/2020

DANIEL ROOT
Special Agent
Federal Bureau of Investigation

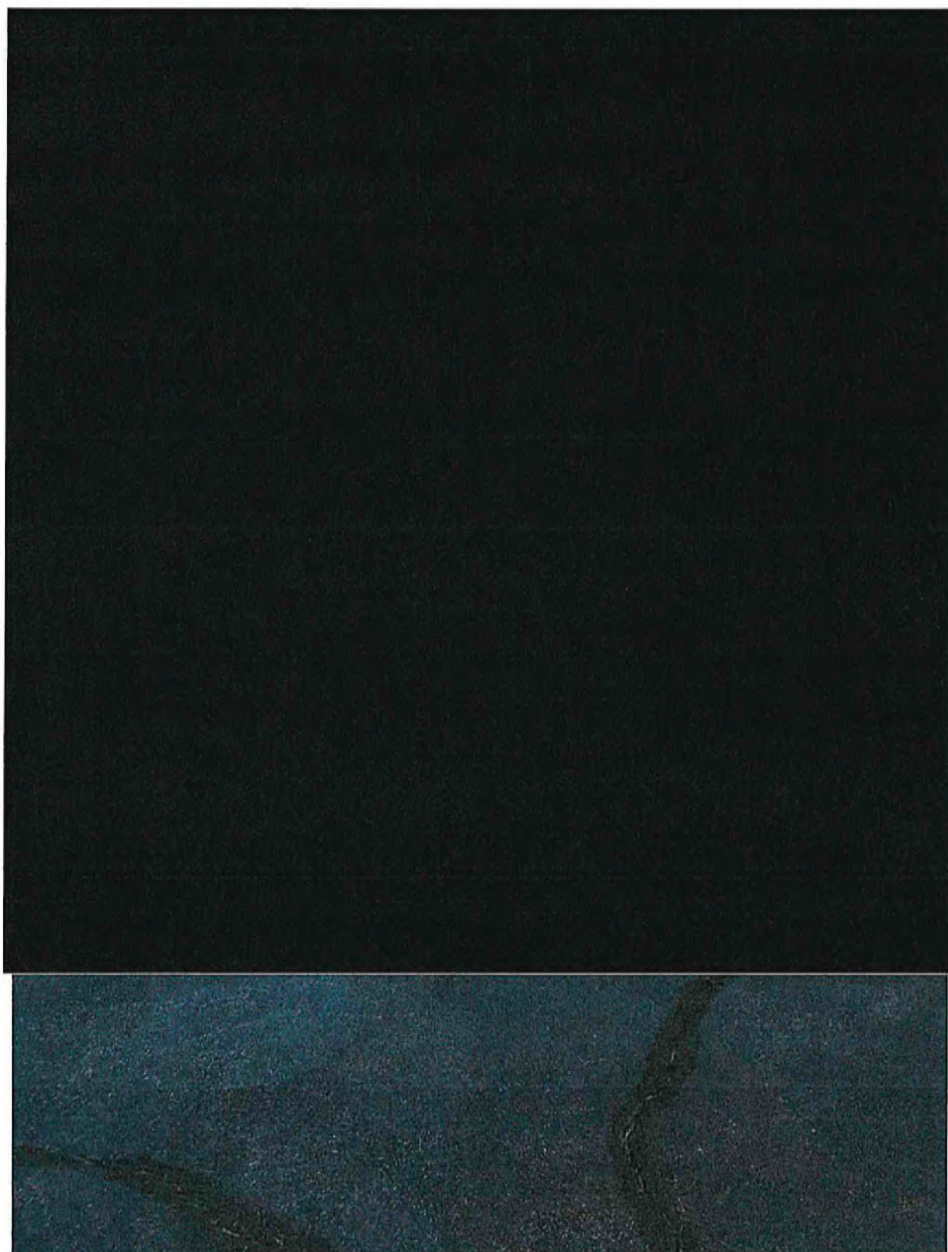
Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 40. this 12th day of NOVEMBER, 2020.


Honorable Noelle C. Collins
UNITED STATES MAGISTRATE JUDGE

4:20 MJ 3301 NCC
ATTACHMENT A
DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire premises located at [REDACTED] Crimson Lane, Barnhart, Missouri, and any person located at the SUBJECT PREMISES.

A two-story structure with a [REDACTED] siding and [REDACTED] brick exterior, with [REDACTED], a [REDACTED] and a shingle-style roof. The numbers "[REDACTED]" are clearly displayed on the front porch post.



4:20 MJ 3301 NCC

ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § § 2251, 2252 and 2252A

- a. Computers or storage media used as a means to commit the violations described above.
- b. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- c. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- d. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence of the lack of such malicious software;
- f. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- g. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- h. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- j. evidence of the times the COMPUTER was used;
- k. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- l. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- m. records of or information about Internet Protocol addresses used by the COMPUTER;
- n. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and contextual information necessary to understand the evidence described in this attachment.
- o. Routers, modems, and network equipment used to connect computers to the Internet.
- p. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
- q. Records, information, and items relating to violations of the statutes described above including:
- r. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, [REDACTED] Crimson Lane, Barnhart, MO, including utility and telephone bills, mail envelopes, or addressed correspondence;
- s. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- t. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- u. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel **BRENT MICHAEL LAWSON** to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICE(S) known to be used by **BRENT MICHAEL LAWSON** that are found at the PREMISES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES’s security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that **BRENT MICHAEL LAWSON** state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

EXHIBIT “3”

4:20-mj-04234

1:19-mj-00830-DJS N.D.N.Y 2019 - Redacted “Boyvid v4”
Search Warrant Affidavit with redactions per Federal Rules of Criminal
Procedure 49.1. Relevant sections highlighted that are common to
Exhibit 1, the “*Kiezjo*” SWA.

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 1)

UNITED STATES DISTRICT COURT
for the
Northern District of New York

BoyVids v4 template



In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
A) Property Located at [REDACTED])
[REDACTED] New Paltz, New York; B) Person)
of Jacob Delaney; and C) Any Computers and)
Electronic Storage Media Located During The)
Searches)

Case No. 1:19-mj-830-DJS

APPLICATION FOR A NO KNOCK SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:
(identify the person or describe the property to be searched and its given location):

See Attachment A

located in the Northern District of New York, there is now concealed
(identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)	Possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, child pornography

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days):

is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature
David Fallon, FBI, Special Agent

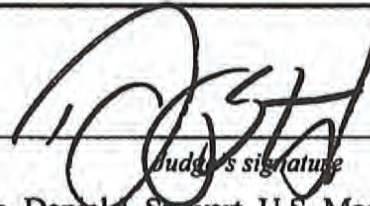
Printed name and title

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 2)

Sworn to before me and signed in my presence.

Date: December 10, 2019

City and State: Albany, NY

A handwritten signature in black ink, appearing to read "D. Stewart", is written over a horizontal line.

Judge's signature

Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, David C. Fallon, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") of the FBI since May 1991, and am currently assigned to the Albany Division. While employed by the FBI, I have investigated federal criminal violations related to child sexual exploitation and child pornography. I have gained experience through training and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child sexual exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am also a member of the FBI's Child Abduction Rapid Deployment Team with extensive specialty training related to conducting, leading, and managing investigations related to missing and abducted children. I also serve as the case agent for the Albany Division's Child Exploitation Task Force which targets online child sexual predators and those individuals who trade child pornography. Prior to becoming employed as a Special Agent, I was an attorney licensed to practice law in the State of Rhode Island. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in

Attachment A of this Affidavit, including (A) the entire property located at 144 Main Street, Apartment 311, New Paltz, New York (the “SUBJECT PREMISES”), (B) the person of Jacob Delaney, and (C) any computers and electronic storage media located during the searches, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. 2252A (possession and access with intent to view child pornography, including the attempt or conspiracy to commit the offense), which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct, or the attempt or conspiracy to commit that offense) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following: 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), which prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, child pornography.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. “Bulletin Board” means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as “internet forums” or “message boards.” A “post” or “posting” is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message “thread,” often labeled a “topic,” refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through “private messages.” Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation.

This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

g. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices

on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

l. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

q. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

r. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

s. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

t. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up

Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on the Tor anonymity network. The website is described below and referred to herein as "TARGET WEBSITE." There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed TARGET WEBSITE, as further described herein.

The Tor Network

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes

communications through the relay computers, traditional IP address-based identification techniques are not effective.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free “Tor browser” from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.¹ The Tor browser is a web browser that is configured to route a user’s Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user’s communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user’s IP address with Tor network relay computers, which are called “nodes.” This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Because a Tor user’s communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an Internet website, only the IP address of the last relay computer (the “exit node”), as opposed to the Tor user’s actual IP address, appears on that website’s IP address log. In addition, the content of a Tor user’s communications are encrypted while the communication passes through the Tor network. That can prevent the operator

¹ Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

13. The Tor Network also makes it possible for users to operate websites, such as those described herein, called "hidden services" or "onion services," in a manner that attempts to conceal the true IP address of the computer hosting the website. Hidden service websites are accessible only to users operating within the Tor network. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view

and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

15. The conduct being investigated involves users of a Tor-network-based website (hereinafter "TARGET WEBSITE") that functioned as an active online forum whose primary purpose was to be a board that was "public, open and free, however, slightly moderate(d) to avoid things that are harmful to the community and / or members, here you can be happy, be yourself and can talk about anything, even controversial issues, but always respecting the rights of other members." The website was dedicated to the sexual exploitation of minor and/or prepubescent males. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. The website launched in approximately 2013 and ceased operating in June 2019. The site allowed users to engage in online communications with other users, either within forums that were openly accessible to any user of the site, within forums only accessible to particular users, or in one-to-one private message chats between two users.

16. The registration page required prospective users to create a user name and password, to identify the user's language and time zone, and to enter a generated confirmation code. By clicking on a user's profile, the date a user joined, total posts, most active forum and most active topic were displayed. The rules listed on the site stated:

- i) Hosts that require javascript, Flash, Java and other plugins to function entirely, may not be linked here.
- ii) It is forbidden to reveal your personal information or personal information of another.
- iii) It is forbidden to sell or trade anything (this includes any offer or request, to send material by Private Messages).
- iv) Constructive criticism is accepted, negative criticism without a solution, are not.
- v) Any language is allowed, but unless writing in the appropriate language sub-forum, an English translation should be provided.

17. Upon entry to the site, users were presented with “announcement,” “rules,” “allowed hosts,” “videos,” and “photos” sections. The “video” and “photo” sections offered links to topics such as “hardcore,” “adolescents,” “toddlers,” “spycam,” “soft hurtcore.” There were descriptions of each topic such as the description for “toddlers” was “0-4 years”, “Fetish” was “cross-dressing, diaper, scat, zoo, etc,” and “soft hurtcore” was “fighting, wrestling, bondage, spanking, etc.”

18. Child pornography images and videos were trafficked through this chat site via the posting of web links within forum messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos are stored, in order to download these image and videos. Entry to the site was obtained through free registration. Users were provided with numerous links to image hosts where users could upload their digital images. For instance, on January 16, 2019, the user “StickItIn” posted a hyperlink of a .jpeg file named “http://i12.pixs.ru/storage/5/7/0/ToddlerBoy_5527045_31141570.jpg”, which depicted an image of a prepubescent male toddler, naked from the waist down with his legs spread apart, having a

bottle inserted into his anus. FBI Special Agents accessed and downloaded child pornography and child erotica files via links that were posted on the TARGET WEBSITE, in an undercover capacity, from computers located in the Eastern District of Virginia.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

19. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the site(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the site is located or the offender appears to reside, in accordance with each country's laws.

20. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on April 22, 2019, a user of IP address 69.206.190.157 accessed online child sexual abuse and exploitation material via a website. FLA described the website as having *"an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys. Users were able to view some material without creating an account. However, an account was required to post and access all content."* FLA

provided further documentation naming the site it described as above as TARGET WEBSITE, which the FLA referred to by its actual name.

21. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

22. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

23. As described herein, TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or 56 character web address of "TARGET WEBSITE" in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory site in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

24. I am also aware through consultation with FBI agents that the review of user data related to one prominent Tor network based child pornography website found that it was

exceedingly rare for a registered site user to access that site and never return. “Playpen” was a Tor network-based hidden service dedicated to the advertisement and distribution of child pornography that operated from August 2014 until March 2015. Similar to TARGET WEBSITE, Playpen was a highly categorized web forum with hundreds of thousands of users. It allowed users to post and download messages pertaining to child exploitation within forum categories indexed by the age and gender of child victims and the type of sexual activity involved. In February and March of 2015, the FBI seized and briefly operated the Playpen website for two weeks, using a court-authorized investigative technique to successfully identify IP addresses and other information associated with site users. FBI review of site data seized from the Playpen website during the operation determined that of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the site and logged in to the same account.

25. Based on my training and experience, because accessing TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

26. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

27. According to publicly available information, IP address 69.206.190.157 which was used to access TARGET WEBSITE on April 22, 2019 was registered to Charter Communications.

28. On November 22, 2019, an Administrative Subpoena was issued to Charter Communications in regard to the pertinent IP address. A review of the results obtained on November 22, 2019 identified the following account holder and address, which is the address of the SUBJECT PREMISES:

Subscriber: Jacob Delaney

Subscriber Address: [REDACTED] New Paltz, NY 12561

Email address: [REDACTED]@hawkmail.newpaltz.edu

Phone number: 631-XXX-XXXX.

29. The email domain [REDACTED].newpaltz.edu corresponds to the State University of New York at New Paltz (SUNY New Paltz). The above listed address, [REDACTED], New Paltz is also known as Paltz Commons, an apartment complex located .4 miles from the SUNY New Paltz campus. Based upon open source information, Paltz Commons is a popular off-campus housing location for SUNY New Paltz students.

30. Open source searches for Jacob Delaney in New Paltz identified a Facebook account. According to the account profile, Jacob Delaney is a student at SUNY New Paltz studying Early Childhood Education.

31. On or about November 22, 2019, a representative of the SUNY New Paltz confirmed that Jacob Delaney is currently enrolled as a graduate student at SUNY New Paltz and lists his address as the SUBJECT PREMISES.

32. Surveillance of the SUBJECT PREMISES on or about November 22, 2019 revealed that [REDACTED], New Paltz is a multi-unit apartment complex. [REDACTED] was located in an entrance way for apartments 309-312. The number [REDACTED] is posted on the door to the SUBJECT PREMISES.

33. On December 3, 2019, a surveillance of the SUBJECT PREMISES was initiated by a member of the New York State Police at the request of your affiant. While engaged in the surveillance, the member observed a person arrive at the SUBJECT PREMISES driving a [REDACTED] Honda Civic, bearing NY license plate [REDACTED]. According to the New York Department of Motor Vehicles, this vehicle is registered to Jacob Delaney. Of note, this member is familiar with the investigative activities in this matter conducted by your affiant and has reviewed the Facebook account of Jacob Delaney. Said account contains images purporting to be of Jacob Delaney. During the surveillance, the member observed a person fitting the description of Delaney exit the Honda Civic and enter the SUBJECT PREMISES at the door labeled for apartments 309-312.

34. According to a New York State repository inquiry, on March 24, 2016, Jacob Delaney submitted an application for employment with the New York State Department of Education.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

35. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four

functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files

on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, ADVERTISE,
TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT
TO VIEW CHILD PORNOGRAPHY**

36. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books,

slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of

forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.²

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices)..

² See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

37. Based on the following, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. For example, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via TARGET WEBSITE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

38. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

40. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file

(such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage

media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this

type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

41. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain

procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

42. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers,

modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

43. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

As White
4949 Brownsboro Rd #247
Louisville, KY 40222

Honorable Judge Hennessy
Harold D. Donohue Federal Building and U.S. Courthouse
595 Main Street
Worcester, Mass 01608